الهيئـــة الـعـامـــة للطيـــران الـمـدنـــي
GENERAL CIVIL AVIATION AUTHORITY

United Arab Emirates

GCAA National Civil Aviation Cybersecurity Strategy (GCAA-NCACSS)

Version 1 - June 2023

رؤيـــتـــنـــا: مـــنـــظـــومـــة طيـــــران مـــدنــــي آمـــنـــة ورائـــــدة ومســـتـــدامـــة
OUR VISION: A LEADING, SAFE, SECURE AND SUSTAINABLE CIVIL AVIATION SYSTEM

Document Control

Record of Amendments			
Version	**Date**	**Reference Section**	**Amendment Content**
1	June 2023	All	Initial Issue

Table of Contents

FOREWORD

Message from the Chairman of the General Civil Aviation Authority (GCAA) Board

The UAE's National Cybersecurity strategy aims to create a safe and strong cyber infrastructure in the UAE that enables its citizens, residents and stakeholders to fulfill their aspirations and empower businesses to thrive in a safe and secure environment. The UAE Cyber Security Council (CSC) responsible for developing and overseeing a cyber security strategy that promotes a secure and resilient cyber infrastructure in the United Arab Emirates and developing a comprehensive cybersecurity strategy and creating a safe and strong cyber infrastructure in the UAE. The strategy is based on 5 pillars and a number of initiatives aiming to mobilize the whole cybersecurity ecosystem in the UAE.

In line with the UAE National Cybersecurity strategy, the General Civil Aviation Authority (GCAA) developed its own civil aviation strategy to combat threats posed by cybersecurity to civil aviation operations in the UAE. This strategy is known as the 'GCAA National Civil Aviation Cybersecurity Strategy'. This new GCAA Cybersecurity Strategy is our plan to ensure that the UAE remains assured, capable and above all resilient in this fast-moving digital world and we continue to adapt, innovate and invest in order to protect and promote UAE's civil aviation interests in the cyber space**.**

His Excellency Abdulla Bin Touq Al Marri
Minister of Economy
Chairman of the General Civil Aviation Authority

Message from the Director General of the General Civil Aviation Authority (GCAA)

I am proud to present the General Civil Aviation Authority's (GCAA's) National Cybersecurity Strategy. This document will guide our collective efforts to prioritize cybersecurity measures within civil aviation over the years ahead.

The GCAA National Cybersecurity Strategy aligns with and supports the UAE National Cybersecurity Strategy. It defines clear pathways to integrate and improve the GCAA's cybersecurity posture, safeguard the civil aviation systems, and build our capacity to meet the ever-changing cybersecurity environment through collaborative partnerships.

With each passing year, the magnitude and volume of cyber threat is increasing rapidly. Cyber-attacks can be damaging as well as extremely expensive for civil aviation operations to endure. In addition to financial damage suffered by the entities, it can also inflict untold reputational damage to any organization. Cyber-attacks these days are becoming progressively destructive and Cybercriminals are using more sophisticated ways to initiate them.

The GCAA National Aviation Cybersecurity vision is to ensure that the Civil Aviation sector in the UAE remains safe, secure, reliable, sustainable and resilient to cyber-attacks. This is achieved by recognizing the obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation, taking into account cybersecurity.

The aim of the GCAA Cybersecurity strategy is for the civil aviation industry to have in place a robust, flexible and dynamic mitigative measures to reduce potential cyber risks, supported by an agreed proportionate regulatory oversight scheme. This will enable civil aviation industry stakeholders to exploit the benefits of cyberspace without compromising aviation safety, security, air navigation and continuity of services.

H. E. Saif Mohammed Al-Suwaidi
Director General of General Civil Aviation Authority of United Arab Emirates

1. Introduction

The civil aviation sector in the UAE and globally is increasingly reliant on the availability of information and communications technology systems, as well as on the integrity and confidentiality of data. The threat posed by possible cyber incidents to civil aviation is continuously evolving, with threat actors focusing on malicious intents, disruptions of business continuity and the theft of information for political, financial or other motivations. Mindful that threats to civil aviation are rapidly and continuously evolving, aviation continues to be a target for perpetrators in the cyber domain as in the physical one, and that cyber threat can evolve to affect critical civil aviation systems worldwide. Aviation cybersecurity covers a wide spectrum of international civil aviation areas such as aviation safety, security, air navigation, and risk management, while giving due consideration to economic, operational and other impacts.

Recognizing the multi-faceted and multi-disciplinary nature of cybersecurity, and noting that cyber-attacks can simultaneously affect a wide range of areas and spread rapidly, it is imperative to develop a civil aviation Cybersecurity Vision and Cybersecurity Strategy.

GCAA National Civil Aviation Cybersecurity Strategy is based on the UAE National Cybersecurity Strategy issued by UAE Cyber Security Council (CSC) and International Civil Aviation Organization (ICAO) Aviation Cybersecurity Strategy.

2. Purpose National Cybersecurity Strategy in the UAE

The purpose of a national cyber security strategy in the United Arab Emirates is to protect the critical infrastructure and information assets of the country from cyber threats and risks. The aviation industry is one of the key sectors that contributes to the GDP and the economic diversification of the UAE, and therefore requires a high level of cyber resilience and security. The national cyber security strategy is aligned with the guidance from the Cyber Security Council and the International Civil Aviation Organization (ICAO), which provide standards and best practices for enhancing the cyber security of the aviation sector. The strategy aims to achieve four main objectives: to establish a robust governance framework for cyber security; to develop the capabilities and skills of the cyber security workforce; to foster a culture of cyber awareness and responsibility among all stakeholders; and to enhance the cooperation and coordination among national and international partners in responding to cyber incidents and challenges.

3. Aviation Cybersecurity Risk Management

Managing cybersecurity risks should:

(i) Draw on aviation safety and security risk management frameworks in order to develop an integrated and accurate assessment of cybersecurity threats and risks, and ensure the development and implementation of effective mitigation measures that take into account safety requirements and the implications of mitigation measures on safety, security and continuity of civil aviation.

(ii) Recognize that not all cybersecurity events affecting the safety of civil aviation are unlawful and/or intentional, there is a need to identify ownership of data and systems at all times. Rules and process should be established by the owners to include physical locations of data and systems, access rights, management rights, and security requirements based on data and system classification. This will support adequate usage of data and systems by the authorized people, setting and implementing quality control standards, and resolving issues and conflicts.

(iii) Consider the need to work collaboratively on an effective and holistic framework to address aviation cybersecurity

(iv) Support the cybersecurity and cyber resilience of the aviation system to cyber threats that may jeopardize the safety or security of civil aviation

4. The UAE Cybersecurity Council (CSC)

The United Arab Emirates Cabinet established the UAE Cybersecurity Council in November 2020 with the aim of developing a comprehensive cybersecurity strategy and creating a safe and strong cyber infrastructure in the UAE. A Memorandum of Understanding related to aviation cybersecurity between the UAE Cabinet Affairs and ICAO was signed in March 2022 enhancing the ICAO-UAE partnership for institutional development and experience exchange. It will see the two parties collaborating more intensively and sharing their knowledge and experience in terms of accelerators, innovation in future civil aviation, and cybersecurity.

The Government set up the CSC to be a single, central body for cybersecurity at a national level. The CSC amongst other things is responsible for:

(a) providing advice and expertise on cybersecurity;

(b) working in cooperation with all relevant entities, industries, academic and international partners to ensure the UAE cyberspace is safe and secure;

(c) analysing, assessing and detecting cyber threats and risks;

(d) managing national cyber incidents;

(e) supporting and advising Government Departments, administrations, regulators, authorities, industries and businesses;

(f) providing cybersecurity expertise to help and support the Government's efforts to foster innovation;

(g) supporting the cybersecurity industry and stimulating the development of cyber security skills; and

(h) providing advice on physical security and personnel security, which forms a part of a multi-layered approach to manage cybersecurity risks.

5. The UAE National Cybersecurity Strategy

The UAE National Cybersecurity Strategy has been developed by UAE Cyber Security Council (CSC) with the Vision to create a safe and resilient cyber infrastructure in the UAE that enables citizens to fulfil their aspirations and empowers businesses to thrive.
Aspirations from the strategy are to:

(i) Provide confidence to citizens to securely participate in the digital world;

(ii) Build a world-class cybersecurity workforce in the UAE;

(iii) Celebrate contributions to innovation in cybersecurity;

(iv) Enable SMEs to safeguard themselves against most common cyber-attacks;

(v) Foster a culture of entrepreneurship in cybersecurity;

(vi) Protect critical information infrastructure assets of the country.

To achieve these aspirations, the UAE mobilizes the whole ecosystem to deliver number of initiatives across 5 pillars such as:

1. Cybersecurity laws & Regulations
(a) Address all types of cybercrimes
(b) Secure existing and emerging technologies
(c) Support protection of SMEs

2. Vibrant Cybersecurity Ecosystem
(a) Support startups and promote R&D in cybersecurity
(b) Develop cybersecurity capabilities
(c) Drive citizen cybersecurity awareness
(d) Encourage excellence in cybersecurity

3. National Incident Response Plan
(a) Single point of contact for victims of cyber incidents
(b) Standardized severity assessment and agency mobilization plan
(c) Cross-agency information sharing

4. CIIP (Critical Infrastructure Information Protection) Programme
(a) Identify critical assets in the UAE
(b) Establish world-class risk management standards
(c) Create robust processes for reporting, compliance and response

5. **Partnerships**
   (a) National Committees
   (b) Local Partnerships
   (c) Global Partnerships

6. International Civil Aviation Organization (ICAO) Aviation Cybersecurity Strategy

ICAO's vision for global cybersecurity is that the civil aviation sector is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow.
The ICAO Aviation Cybersecurity Strategy aligns with other cyber-related ICAO initiatives in coordination with corresponding aviation safety and aviation security management provisions. The Strategy's aims will be achieved through a series of principles, measures and actions contained in a framework built on seven pillars:

(i) International cooperation

(ii) Governance

(iii) Effective legislation and regulations

(iv) Cybersecurity policy

(v) Information sharing

(vi) Incident management and emergency planning

(vii) Capacity building, training and cybersecurity culture

7. The GCAA National Aviation Cybersecurity Vision

The GCAA National Aviation Cybersecurity Vision is: "Civil Aviation sector in the UAE to remain safe, secure, reliable, sustainable and resilient to cyber-attacks".

This can be achieved through:

(i) recognizing the obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation, taking into account cybersecurity;

(ii) recognizing the initiative of the Dubai Declaration on cyber security in civil aviation and the ICAO Assembly Resolution A40-10 reaffirming the importance and urgency of addressing cybersecurity and cyber resilience of civil aviation critical systems, data and information against cyber threats and hazards;

(iii) coordination of aviation cybersecurity amongst relevant national authorities to ensure effective and efficient management of cybersecurity risks; and

(iv) commitment by civil aviation stakeholders in the UAE to further develop cyber resilience, protecting against cyber-attacks that might impact the safety, security and continuity of the air transport systems.

8. Overall General Civil Aviation Authority Strategy

The General Civil Aviation Authority strategic objectives set out the long-term direction for aviation policy making for 2050 and beyond. They are:

(i) Development and enforcement of safety and security regulations according to the international standards and best practices.

(ii) Continuous improvements of the safety and service standards in the provision of air navigation services.

(iii) Elevate UAE aviation in the global arena.

(iv) Continuous improvements in the bi-lateral relations.

(v) To ensure that GCAA services are provided according to the standards of quality efficiency and transparency.

(vi) Instill innovation culture within the corporate working environment.

This GCAA National Civil Aviation Cybersecurity Strategy will directly contribute to achieving the above-mentioned objective (i). It will also facilitate objectives (ii), (iii) and (vi) by supporting development of the regulatory environment and technological advancement.

9. The GCAA Cybersecurity Taskforce

The aim of the GCAA Cybersecurity Taskforce is for industry to have in place a robust, flexible and dynamic mitigations to reduce potential cyber risks, supported by an agreed proportionate regulatory oversight scheme. This will enable all aviation industry stakeholders to exploit the benefits of cyberspace without compromising aviation safety, security, air navigation and continuity of services.

9.1 GCAA National Civil Aviation Cybersecurity Strategy Objectives

9.1.1 Objectives of the GCAA National Civil Aviation Cybersecurity Strategy are:

(i) Foster cybersecurity culture in civil aviation.

(ii) Enable civil aviation stakeholders to safeguard themselves against common cyber-attacks.

(iii) Require stakeholders to identify and protect critical information and communications technology systems and data used for civil aviation purposes, including infrastructure and assets of the country.

(iv) Develop sufficient human resources, capacity and capability by delivering appropriate, coherent and relevant aviation cybersecurity training for personnel of the appropriate authority for aviation cybersecurity and relevant stakeholders.

(v) Ensure business continuity related to cybersecurity.

(vi) Provide confidence to aviation stakeholder and the travelling public to securely participate in the digital world.

(vii) Contribute to innovation in cybersecurity.

9.1.2 To achieve the stated objectives through this Strategy, the overarching principles are:

(i) Understanding the risks posed by cyber threats to and vulnerabilities within the aviation sector, and its potential consequences;

(ii) Managing cyber risks and taking appropriate and proportionate action to protect key assets;

(iii) Responding to and recovering from cyber events and incidents effectively and ensure that lessons are learnt;

(iv) Promoting cultural changes, raising awareness and building cyber capability.

10. Pillars of GCAA National Civil Aviation Cybersecurity Strategy

The GCAA National Civil Aviation Cybersecurity Strategy aligns with UAE national Cybersecurity pillars and ICAO initiatives and pillars in coordination with corresponding aviation safety and aviation security management provisions. This Strategy are to be achieved through a series of principles, measures and actions contained in a framework built on seven pillars:

1. International cooperation & partnership
2. Governance
3. Effective legislation and regulations
4. Cybersecurity policy
5. Information sharing
6. Incident management and emergency planning
7. Capacity building, training and cybersecurity culture

1. International Cooperation & Partnership

1.1 GCAA supports the harmonization of aviation cybersecurity at the global, regional and national levels in order to ensure consistency and full interoperability and risk management system. Cybersecurity and aviation are both borderless in nature. GCAA shall support cooperation at the national and international level and call for a mutual recognition of efforts to develop, maintain and improve cybersecurity with the aim to protect the civil aviation sector from all cyber threats to safety and security.

1.2 GCAA will support the development of effective partnerships with public and private sectors as required.

2. Governance

2.1 Develop clear national governance and accountability according to UAE Cyber Security Council (CSC) requirements concurrently with ICAO cyber security roadmap.

2.2 Develop clear national governance and accountability for civil aviation cybersecurity by designating the GCAA as the Appropriate Authority for Aviation Cybersecurity in the UAE with an overall mandate and responsibility for aviation cyber security and cyber resilience.

2.3 Define roles and responsibilities to be undertaken by relevant entities and stakeholders related to Civil Aviation Cyber Security.

2.4 The designated Appropriate Authority for Aviation Cybersecurity shall ensure coordination with relevant civil aviation and cybersecurity stakeholders by establishing appropriate coordination channels.

2.5 The GCAA National Aviation Cybersecurity Strategy shall be the basis for the stakeholders to develop their respective civil aviation cybersecurity strategies to ensure the safety, security and continuity of civil aviation in an environment jeopardized by cybersecurity threats.

3. Effective Legislation and Regulation

3.1 Ensure that appropriate legislation and regulations are based on ICAO provisions and maintained accordingly. Further development of appropriate guidance for stakeholders and industry in implementing cybersecurity related provisions. GCAA is committed to create, review and amend, as appropriate, guidance material relating to the inclusion of cybersecurity aspects to security and safety.

3.2 Support the development and implementation of this comprehensive Cybersecurity Strategy to protect civil aviation and the travelling public from the effects of cyber-attacks by the development of Aviation Cybersecurity legislation and regulations harmonized on international, regional and national level.

3.3 Support development of relevant international legal instruments addressing key legal provisions for the prevention, prosecution, and timely reaction to cyber-incidents in order to form the basis for consistent and coherent implementation of cybersecurity legislation and regulations throughout the global aviation sector.

3.4 Support further development of national legislation for the prosecution of evolving terrorist- related cyber threats as well as cyber-attacks impacting civil aviation.

3.5 Include provisions on aviation cybersecurity in the national civil aviation safety and security programmes in accordance with ICAO SARPS.

4. Cybersecurity Policy

4.1 Support and encourage the development of cybersecurity policies such as: cybersecurity culture, promotion of security by design, supply chain security for software and hardware, data integrity, appropriate access control, pro-active vulnerability management, improving agility in security updates without compromising safety, as well as incorporating systems and processes to monitor cybersecurity relevant data.

4.2 Include cybersecurity within GCAA's aviation security and safety oversight systems as part of a comprehensive risk management framework.

4.3 Further develop guidance material related to cybersecurity threat and risk assessments with the aim to achieve comparability of the outcomes of such assessments bearing in mind the different risk assessment methodologies.

4.4 Align with the UAE Critical Information Infrastructure Protection (CIIP) Policy issued by the UAE Cyber Security Council (CSC)

5. Information Sharing

5.1 Support a culture of information sharing to allow for prevention, early detection and mitigation of relevant cybersecurity events before they lead to wider effects on aviation safety or security. Reduce systemic cyber risk across the aviation sector by implementing a culture of information sharing the value of which has already been proved across aviation safety and security.

5.2 Reduce the impact of ongoing attacks by sharing information on such aspects as vulnerabilities, threats, events and best practices, through established and trusted channels in line with ICAO provisions.

6. Incident Management and Emergency Planning

6.1 Coordinate the Incident management and emergency planning with the Cyber Security Council (CSC) to meet the national cybersecurity requirements.

6.2 Ensure continuity of air transport during cyber incidents by including appropriate and scalable cybersecurity plans in the existing incident management mechanisms. Amend the existing Contingency Plans to include provisions for cybersecurity.

6.3 Encourage the conduct of cybersecurity exercises (table-top exercises, simulations or real-time exercises), which is a useful tool to test cyber resilience and identify improvements.

7. Capacity Building, Training and Cybersecurity Culture

7.1 Increase the number of personnel qualified and knowledgeable in both aviation and cybersecurity because the human element is critical as well as the core of cybersecurity. Enhance awareness of cybersecurity, as well as education, recruitment and training. Include in the national educational framework and training programmes curricula relevant to cybersecurity and where practical aviation-specific cybersecurity at all levels.

7.2 Support and stimulate skills development in the existing and new workforce to enable fostering of cybersecurity innovation and appropriate research and design in the aviation sector. Ensure appropriate job-related training on a continuous basis to support personnel in their daily roles.

7.3 Include cybersecurity in the strategy for the next generation of aviation professionals based on ICAO initiatives to develop role-based competency requirements for aviation professionals.

7.4 Apply principles of proactive safety and security culture to develop and maintain a cybersecurity culture across the aviation sector making it everybody’s responsibility.

- End of Document -